MMRA is pleased to provide our customers with a presentation which will address the modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules which was released on January 25, 2013.
• The final rules were released to modify HIPAA Rules and implement statutory amendments under the HITECH Act. These rules strengthen the privacy and security protection for individual health information; modifies the rule for Breach Notification for Unsecured PHI and strengthens the HIPAA Privacy Rule for genetic information (GINA).
• The Effective date of this final rule is March 26, 2013.
• Covered entities and business associates must comply with the requirement of the final rule by September 23, 2013.
Access of Individuals to Protected Health Information

If the individual requests an **electronic copy** of PHI that is **maintained electronically**, the covered entity **MUST** provide the individual with access in the form or format requested.

• Section 164.524 of the Privacy Rule permits individuals the right to review or obtain copies of their PHI. This right currently exists regardless of the form or format of the PHI. The HITECH Act strengthens the Privacy Rule’s right of access by addressing the covered entities whom use or maintain an electronic health record.
• Thus, the final rule requires that if an individual requests an electronic copy of PHI that is maintained electronically in one or more designated record sets, the covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual. The expectation is that the covered entity will provide the individual with “machine readable” copy of their PHI. Machine readable means digital information and includes formats of MS Word or Excel, text, HTML, or text-based PDF, among others.
Individual Access: Form and Format
164.524 (a)

* Covered entity is required to provide electronic information to the individual in the electronic form and format requested.
  - Covered entity and individual must agree to the format
  - If individual declines to accept the format the covered entity has available, hard copy may be offered as an option
  - Hard copy does not satisfy the electronic access request unless the individual does not accept the format offered
  - Covered entity is not required to scan paper to provide electronic copy

- As was mentioned earlier, the HITECH Act expanded the requirement of allowing patients access to their PHI by requiring a covered entity that uses or maintains an EHR with respect to PHI to provide the individual with a copy of such information in an electronic format.
- The privacy rule was modified to state that a covered entity is required to provide electronic information to an individual in the electronic form and format requested by the individual. Obviously, the electronic form and format will vary by system; therefore, the covered entity is allowed to provide the electronic copies of the PHI that are currently available. A covered entity is not required to purchase new software or systems in order to accommodate an electronic copy request for a specific form that is not readily producible at the covered entity at the time of the request, provided that the covered entity is able to provide some form of electronic copy. There may be older or legacy systems that may not have the capability to provide the information electronically and some investment may have to be made by the covered entity to provide the information electronically.
- Covered entities need to provide individuals with some kind of readable electronic copy but can limit the type of electronic copy. If the individual requests a form and format that the covered entity cannot produce, the covered entity must offer another type of electronic copy. However, if the individual declines to accept any of the electronic formats that the covered entity is able to produce, a hardcopy may be provided as an option to fulfill the request for information. Please note that a hard copy of the PHI would not suffice the requirement unless the individual decides not to accept any of the electronic formats offered by the covered entity.
- The electronic copy must reflect all electronic PHI maintained by the covered entity in a designated record set. It is important to note that the covered entity is not required to scan paper documents to provide electronic copies of records maintained in hard copy. It can be scanned...but not required.
- Covered entities are not required to use portable devices that the individual might bring with them such as flash drives. If the covered entity does not allow for the format that individual has requested, an alternate electronic form must be offered.
- Covered entities are permitted to send individual unencrypted emails if that have advised the individual of the risk and the individual still prefers the unencrypted email. Each facility should determine what their policy will be on the types of form and formats to offer individuals.
- Covered entity not required to purchase new software or systems
Access of Individuals: Third Parties
164.524 (b)

* If requested by an individual, a covered entity must transmit the copy of PHI directly to another person designated by the individual.

* Request must be made in writing

• In concert with the HITECH Act, HIPAA requires that if an individual requests a covered entity to transmit the copy of PHI directly to another person designated by the individual. 
• The rule requires the requests to be made in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the PHI. The rule does not require this written request to be a HIPAA compliant authorization form, but your facility may require the authorization as the written request.
• The Privacy Rule currently permits a covered entity to charge a reasonable, cost-based fee for a copy of PHI. However, the fee may only include the cost of supplies for and labor of copying the PHI, postage, and the preparation of the information. The HITECH Act stated that a covered entity may not charge more than its labor costs in responding to the requests.

• The final rule states the covered entity may charge a fee the identifies separately the labor for copying PHI, whether in paper or electronic form. The labor costs include a reasonable cost-based fee which includes skilled technical staff time spent to create and copy the electronic file such as compiling extracting, scanning and burning PHI to media and distributing the media. It also includes the time spent preparing the information.

• The final rules also allows the covered entity to provide separately the cost of supplies for creating the paper copy of electronic media. Supplies for electronic media may include the CD/DVD, flash drive, etc., if the individual requests the information to be provided on such electronic media. New technology is not required to be purchased to satisfy the individual’s request.

• The covered entity may continue to charge postage for the mailing for the electronic form. A handling fee cannot be charged to individuals as is the current rule.

• When State laws designate fees and limits on those fees, a covered entity may charge these fees as they are considered “reasonable”. The rule states that the fees charged must be reasonable and cost-based.

• A certification fee may continue to be charges as applicable; this is not required to be part of the copying fee.

• A covered entity may not withhold an individual’s copy of his or her PHI for failure by the individual to pay any fees for services.
Access of Individuals: Timeliness 164.524 (d)

- Maintains 30 day TAT
- Maintains the one-time extension of 30 days
- Removes 60 days from timely action when PHI for access is not maintained or accessible to the covered entity on-site
- Maximum of 60 days instead of 90 days.

The final rule removes the provision which permits 60 days for timely action when PHI is not maintained or accessible to the covered entity on-site. It retains the one-time extension of 30 days to respond but removes the additional 30 days. It is believed that the 30 days timeframe for access is sufficient given the increasing use of electronic records. Covered entities are encouraged to provide individuals with access to their information sooner than permitted.

Please note that this rule does not supersede the CMS incentive program requirement (Meaningful use).
The privacy rule was amended to require a covered entity to comply with the Rule with regard to PHI of a deceased individual for a period of 50 years following the date of death. Thus, individually identifiable health information of a person who has been deceased for more than 50 years is not PHI under the Privacy Rule.

If there is State or other laws that provide greater protection for such information, those rules supersede the privacy rule. This is not to be considered a record retention requirement; it’s only in effect if the information is maintained.
• The Privacy Rule amended this section to add that a covered entity is permitted (but not required) to disclose a decedent’s PHI to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual if known by the covered entity. Another exception is if the individual, prior to his/her death, objected to the covered entity making such communications.
• A personal representative would continue to have a right to access the decedent's PHI as appropriate, and have authority to authorize uses and disclosures of the decedent’s PHI that are not otherwise permitted or required by the privacy rule.
Disclosure of Student Immunizations to Schools

164.512 (b)

* A covered entity is permitted to disclose proof of immunization to a school where State or other law requires the school to have such information prior to admitting the student.

* Written authorization is no longer required; must obtain agreement from parent/guardian.

* Must document the agreement

• The privacy rule is being amended to add that a covered entity to disclose proof of immunization to a school when it’s required by the State to show such proof prior to being admitted as a student. Written authorization is no longer required, however the covered entity must obtain and document an agreement. The agreement may be oral, from a parent, guardian or other person acting in loco parentis for the individual or from the individual him/herself.

• The documentation is determined by the facility and rule does not require a patient signature. A copy of the request would suffice as documentation of the agreement. Filing this agreement or making a notation in the medical record is considered documenting the agreement. A documented phone call would also suffice.

• Please note: a request by a school for the immunization records is not permitted. The parent must request and or approve.
Right to Request Restriction
164.522 (a)

* Covered entity must agree to restriction of releasing information to a health plan IF individual pays the health care provider out of pocket in full for item or service.
* Must note the information is restricted.

• Even though the Privacy Rule allows the covered entity to deny a request for restriction, the HITECH Act sets forth circumstances in which a covered entity now must comply with an individual’s request for restriction of disclosure of his or her PHI.
• The HITECH Act requires that when an individual requests a restriction the covered entity must agree to a restriction when such restriction applies to disclosures of PHI that pertains solely to a health care item or service for which the health care provider has been paid out of pocket in full.
• If a provider is required by State or other law to submit a claim to a health plan for a covered service provided to the individual and there is no exception or procedure for individual wishing to pay out of pocket for the service, then the disclosure is required by law and is an exception to an individual’s right to request a restriction to the health play.
Clarification of definition of Breach 164.402 (a):

An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or BA demonstrates that there is a low probability that the PHI has been compromised.

• The HITECH Act requires covered entities to provide notification to affected individuals and to the Secretary of HHS, and the media is come some cases, upon discovery of a breach of PHI. The final rule addresses such notification plus definition of breach.
• Definition of breach is amended as such: is the unauthorized acquisition, access, use or disclosure of PHI which compromised the security or privacy of such information.
• There are three exceptions to the definition: 1) Unintentional—if access was made in good faith; 2) inadvertent disclosure; and 3) unauthorized disclosures in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.
• The final rule modifies and clarifies the definition of breach and the risk assessment approach.
• It first adds language to the definition of breach to an impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised. The breach notification is necessary unless the covered entity and business associate can demonstrate that there is a low probability that the PHI has been compromised. The covered entity or business associate has the burden of proof.
Next, the final rule removed the “harm” standard and focuses more objectively on the risk that the PHI has been compromised. Thus, the notification is not required if the risk assessment concludes that there is a low probability that the PHI has been compromised.

The final rule states that the covered entity and/or business associate should conduct a risk assessment and include the following steps:

1) Evaluation the nature and type of PHI compromised including the types of identifiers and the likelihood of re-identification whether or if the information is of a more sensitive nature (type of PHI involved such as diagnosis, treatment, medication and financial info like social security number and credit card numbers; will the nature and type of information disclosed have an adverse affect on the individual if used in an unauthorized manner.

2) Consider the unauthorized person receiving PHI or to whom the impermissible disclosure was made (does the unauthorized person who impermissibly used the PHI or whom the disclosure was made have an obligation to protect the privacy and security of such information?)

3) Investigate whether the PHI was actually viewed or if the opportunity existed for the information to be acquired or viewed;

4) Attempt to mitigate the risks to the PHI following any impermissible use or disclosure, such as by obtaining the recipient’s satisfactory assurances that the information will not be further used or disclosed or will be destroyed and should consider the extent and efficacy of the mitigation. (the covered entity and business associates should attempt to mitigate the risks to the PHI such as contract the recipient to return or destroy information and whether or not they can rely on such assurances.

If an evaluation of these factors fails to demonstrate that there is a low probability that the PHI has been compromised, breach notification is required.

Covered entities and business associates should examine their policies to ensure that when evaluating the risk of an impermissible use or disclosure they consider all of the required factors. There may be additional factors that may be taken under consideration in order to appropriately assess the risk that the PHI has been compromised.
The HITECH Act defines unsecured PHI as PHI that is not secured through use of technology or methodology specified by the Secretary of HHS. Changes “unauthorized individuals” to “unauthorized persons”.
Individuals whose PHI may have been breached must be notified not later than 60 calendar days from the discovery of the breach.

“Discovered” is considered the first day on which the breach is known or should be reasonably known.

The HITECH Act provides that a covered entity must notify each affected individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been access, acquired, or disclosed is a result of such breach. The privacy rule is adopting this requirement.

A breach is to be treated as discovered by a covered entity or business associate if “any person, other than the individual committing the breach, that is an employee, officer or other agent of such entity or associate knows or should reasonably have known of the breach.”

The privacy rule also upholds the HITECH Act content of the notification items, timeliness of the notification (60 calendar days from the discovery of the breach except where certain law enforcement has request a delay).

All covered entities and business associates are encouraged to ensure their workforce are adequately trained on the importance of prompt reporting of privacy and security incidents.

Content requirements of the Notification to Individuals are as such:

1) Brief description of what happened, including the date of the discovery of the breach
2) Description of the types of unsecured PHI that were involved in the breach (name, social security number, diagnosis)
3) Steps the individuals should take to protect themselves from potential hear resulting from the breach
4) Brief description of the investigation the covered entity is engaged in in order to mitigate harm to the individual(s) and protect against further breaches of the same nature
5) Contact information for the individuals to ask questions or get more information
• As required by the HITECH Act, the final rules retain the requirement that a covered entity must provide notice of a breach to prominent media outlets in a state or jurisdiction, following the discovery of a breach if the unsecured PHI of more the 500 residents of such state or jurisdiction. The media notice is in addition to the notification of the individuals in which the breach affected.
• The media must be notified no later than 60 calendar days after discovery of the breach. Content of the notification is the same as the content to the individual.
• If the breach involves more than 500 individuals who are residents in multiple states, media notification is only required if there are more than 500 individuals from one particular state. For example—if there are 300 individuals from Illinois affected and 300 individuals from Wisconsin affected, this is less than 500 in one state, thus the media does not need to be notified.
• This rule does not require a covered entity to incur any cost to print or run media notice about a breach of unsecured PHI nor does it require media outlets who receive the notice to print or run the information. A press release sent to prominent media outlets in the state or area would suffice.
For breaches affecting more than 500 individuals, Secretary must be notified immediately.

Covered entities are required to notify the Secretary of all breaches of unsecured PHI affecting fewer than 500 individuals not later than 60 days after the end of the calendar year in which the breach was discovered.

As required by the HITECH Act, the final rules retain the requirement that a covered entity must notify the Secretary of HHS of breaches of PHI. For breaches affecting 500 or more individuals, the Secretary must be notified immediately. Immediately is defined as notification should be sent concurrently with the notification sent to the individual.

For breaches affecting fewer than 500 individuals, a covered entity must notify the Secretary not later than 60 days after the end of the calendar year in which the breaches occurred—not in which the breaches occurred.

Again, this notification to the Secretary is in addition to notifying the individuals affected by the breach.
Notification by a Business Associate 164.410

* BA’s required to notify the covered entity of breach upon discovery
* Must provide notification to covered entities no case later than 60 days from discovery of the breach
* Must provide the identity of each individual whose unsecured PHI has been affected.
* Covered entity is responsible for providing notice to individuals affected.

• A business associate is required to provide notification of a breach to the covered entity no later than 60 days from discovery of the breach. The business associate must provide the covered entity with the identity of each individual, to the extent possible, and other required content, whose PHI has or is reasonably believed to have been breached.
• The covered entity is responsible for notifying the individual(s) of the breach.
• “To the extent possible” means that there may be cases in which the business associate may not know the identity of the individuals affected and can therefore only provide as much information as possible.
* If law enforcement determine that notification of a breach would impede a criminal investigation, the notification can be temporarily delayed
* Delay must be in writing to the covered entity from law enforcement
* Delay should be no longer than 30 days

If a law enforcement official determines that notification of a breach could impede a criminal investigation or cause damage to national security, the notification may be temporarily delayed. Law enforcement officials must provide a statement in writing stating such, plus the time for which a delay is required. The covered entity is required to comply with the delay. The delay of the notification should be no longer than 30 days.
Covered entities and business associates must ensure that all workforce members are trained and knowledgeable about what constitutes a breach and reporting of such.

The Privacy provisions require that covered entities and business associates must ensure that all workforce members are trained and knowledgeable about what constitutes a breach and reporting of such.

Policies and procedures must be reviewed and updated as appropriate and train the affected workforce. The covered entity must also include sanction for failure to comply with the policies and procedures set forth by the covered entity.
* BA’s are directly liable for impermissible uses and disclosures for
  * Failure to provide breach notification to the CE
  * Failure to provide access to a copy of electronic PHI to either the covered entity, the individual, or the individual’s designee
  * Failure to disclose PHI where required by the Secretary
  * Failure to provide an accounting of disclosure
  * Failure to comply with the requirement of the Security Rule

• Before the HITECH Act, the Privacy Rule did not directly include business associates. The HITECH Act specifies that business associates are directly liable for impermissible uses and disclosures of PHI as stated in the Privacy Rule.
• Thus, 164.502 is modified to provide that a business associate may not use or disclose PHI except as permitted or required as specified in the business associate contract.
• Business associate are directly liable under the HIPAA Rules for impermissible uses and disclosures; for a failure to provide breach notification to the covered entity; for a failure to provide access to a copy of electronic PHI to either the covered entity, the individual; failure to disclose PHI where required by the Secretary; for failure to provide an accounting of disclosure; and, for failure to comply with the requirements of the Security Rule.
Business Associates
164.502 (e)

* Definition modified to include any entity that “creates, receives, maintains or transmits” PHI on behalf of covered entity
* BA’s are directly liable for impermissible uses/disclosure of PHI

• Business Associates are now defined as any entity that creates, receives, maintains or transmits PHI on behalf of a covered entity. Therefore, business associates are now directly liable for civil money penalties under the HIPAA Privacy Rule specific to impermissible uses and disclosure of PHI.
Minimum necessary standard applies to business associates.

- The minimum necessary standard applies directly to business associates when using or disclosing PHI or when requesting PHI from another covered entity.
• HIPAA section 164.502 (e) permits a covered entity to disclose PHI to a business associate and may allow a business associate to create or receive PHI on its behalf via a written contract between the two parties.
• The final rule also allows for subcontractors to create or receive PHI on the behalf of the covered entity and therefore must also have a written agreement or contract. This also extends to business associate to return or destroy all PHI received from, or created or received on behalf of, the covered entity at the termination of the contract.
Covered entities, BA and BA subcontractors are allowed to continue to operate under certain existing contracts for up to one year beyond the compliance date of the revision to the Rules.

The final rule adopts new transition provisions to allow covered entities and business associates, including subcontractors, to continue to operate under certain existing contracts for up to one year beyond the compliance date of the revisions to the Rules. If there are agreements in place that were negotiated to meet the HITECH Act, covered entities should review these contracts to assure that they meet the final rules provisions. If they do not, the covered entity has the one year transition period to make the necessary changes.
* Sale of PHI is prohibited unless an authorization is obtained.
* Definition for the sale of PHI clarified:
  * “disclosure of PHI by a covered entity or business association where the covered entity or business associate directly or indirectly received remuneration from or on behalf of the recipient of the PHI in exchange for PHI”
  * Remuneration means both financial and nonfinancial benefits (in-kinds benefits)

• Current privacy rule section 164.508 permits a covered entity to use and disclosure PHI WITH a valid authorization for the following circumstances: most uses and disclosure of psychotherapy notes and uses and disclosures for marketing purposes.
• The HITECH Act added another circumstance in which an authorization is required to be obtained from the individual: the Sale of PHI.
• The final rule adopts the HITECH Act provision which prohibits the sale of PHI by a covered entity or business associate.
• The rule also further defines “sale of PHI” as if a covered entity or business associate receives compensation or payment from the exchange of PHI. This includes nonfinancial benefits as well such as gift in-kind.
• Therefore, a covered entity is required to obtain an authorization for any disclosure of PHI in which there is an exchange for direct or indirect compensation or payment (remuneration) from or on behalf of the recipient of the information.
Uses and Disclosures Requiring Authorization: Research

164.508

*Rule was amended to allow compound authorization for research.
*Must clearly state the individual is allowed to opt out of the unconditioned research activities.
*Does not include research involving psychotherapy notes.

• The HIPAA Rule adopts the amendment to 164.508 to allow a covered entity to combine conditioned and unconditioned authorization for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research and clearly allow the individual the option to opt in to the unconditioned research activities.
• For research that involves the use or disclosure of psychotherapy notes, an authorization of those notes may only be combined with another authorization for use or disclosure of psychotherapy notes.
• The Privacy Rule has made a number of changes to the fundraising requirement. First, in addition to demographic information, health insurance status and dates of health care provided, the categories of PHI of the individual that may be used or disclosed now includes the department in which service was rendered (i.e. cardiology, oncology, etc.); treating physician information and outcome information. Outcome information includes information regarding the death of the patient or any sub-optimal result of treatment of services.

• Additionally, the provision strengthens the opt-out language. It states that the covered entity cannot impose an undue burden on the individual to opt out of fundraising. In other words, covered entities should provide a reasonable method for the individual to opt-out of fundraising communications such as a toll-free phone number to call, an email address to contact or anything that is simple, quick and inexpensive.

• The covered entity can also not condition treatment or payment on the individual’s choice of fundraising communications and the Notice of Privacy Practices must clearly inform individuals that a covered entity may contact them to raise funds for the covered entity and an individual has a right to opt out of receiving such communications. The covered entity but also provide individual with choice to opt-out of all future fundraising communications.
Additional statements to be added:
* description of the uses and disclosure of PHI that require authorization
* uses and disclosures of psychotherapy notes, PHI for marketing purposes and sale of PHI all require authorization
* the individuals right to opt out of receiving fundraising communications
* inform individuals of their new right to restrict certain disclosure when paying out of pocket
* the individuals right of notification of a breach of unsecured PHI in which they were affected.

• The Notice of Privacy Practice for providers will need to be revised as there have been a few changes.
• The provision which addresses the Notice of Privacy Practice now requires statements regarding the use and disclosure that require authorization. The Rule does not require the covered entity to list all situations requiring authorization but must include a statement indicates that most uses and disclosure of psychotherapy notes, uses and disclosure of PHI for marketing purposes, and disclosure that constitute a sale of PHI require authorization. A statement that other uses and disclosure not described in the NPP will be made only with authorization from the individual.
• The Notice also requires a statement regarding fundraising communications and an individual’s right to opt out of receiving such communications if the covered entity intends to contact the individual.
• The new right to restrict certain disclosures of PHI to a health plan when the individual pays out of pocket in full for an item or service also need to be addressed.
• The Notice must also include the right that the individual is to be notified following a breach of PHI in which the individual may have been affected.
• Providers do not need to re-distribute the NPP containing these revisions. The revisions must be posted and new patients must still receive a NPP.
• **GINA (Genetic Information Nondiscrimination Act of 2008)** prohibits discrimination based on an individual’s genetic information for both health insurance coverage and employment.
• The Privacy final rule prohibits the use or disclosure of PHI that is genetic information for underwriting purposes to all health plans that are HIPAA covered entities.
• It is also prohibited to use with underwriting for group health plans, health insurance issuers, health maintenance organizations and issuers of Medicare supplemental policies.
• Long term care policies are exempt.

- Prohibits all health plans, health and insurance issuer from using or disclosing PHI for underwriting purposes
- Includes group health plan, health insurance issuer of Medicare supplemental policy.
Civil Monetary Penalty

<table>
<thead>
<tr>
<th>Violation</th>
<th>Each Violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know</td>
<td>$100 - $50,000 per violation ($1.5 million cap)</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 - $50,000 ($1.5 million cap)</td>
</tr>
<tr>
<td>Willful neglect/corrected</td>
<td>$10,000 - $50,000 ($1.5 million cap)</td>
</tr>
<tr>
<td>Willful neglect/uncorrected</td>
<td>$50,000 ($1.5 million cap)</td>
</tr>
</tbody>
</table>

• 164.404 has been revised specific to the range of potential civil money penalty amounts a covered entity or business associate will be subject to for violations occurring on or after February 18, 2009.
• For violations in which the covered entity would not have known that the covered entity was in violation of a provision, the amount of penalty is no less than $100 or no more than $50,000 for each violation.
• In the case of a violation was due to reasonable cause and not willful neglect, the penalty amount is not less that $1,000 but no more than $50,000 for each violation.
• For a violation which was determined was due to willful neglect and was timely corrected, the penalty amount is not less than $10,000 but no more than $50,000.
• For a violation in which it was determined was due to willful neglect and was not timely corrected, an amount not less the $50,000 for each violation.
• No violation may exceed $1,500,000 in a calendar year.
• Actual penalty amounts will be determine based on the nature and extent of the violation, the nature and extent of the resulting harm.
Questions?

Contact your Regional Manager,
Director of Operations
or Sales Representative.

(800) 930-6672 | info@mmrainc.com
| www.mmrainc.com | https://twitter.com/mmrainc